Cross Device Flows

Pieter Kasselman Daniel Fett Filip Skokan

IETF 115 London (Nov 2022)
Date: 9 Nov 2022


MIND THE GAP

Today’s Discussion

The problem

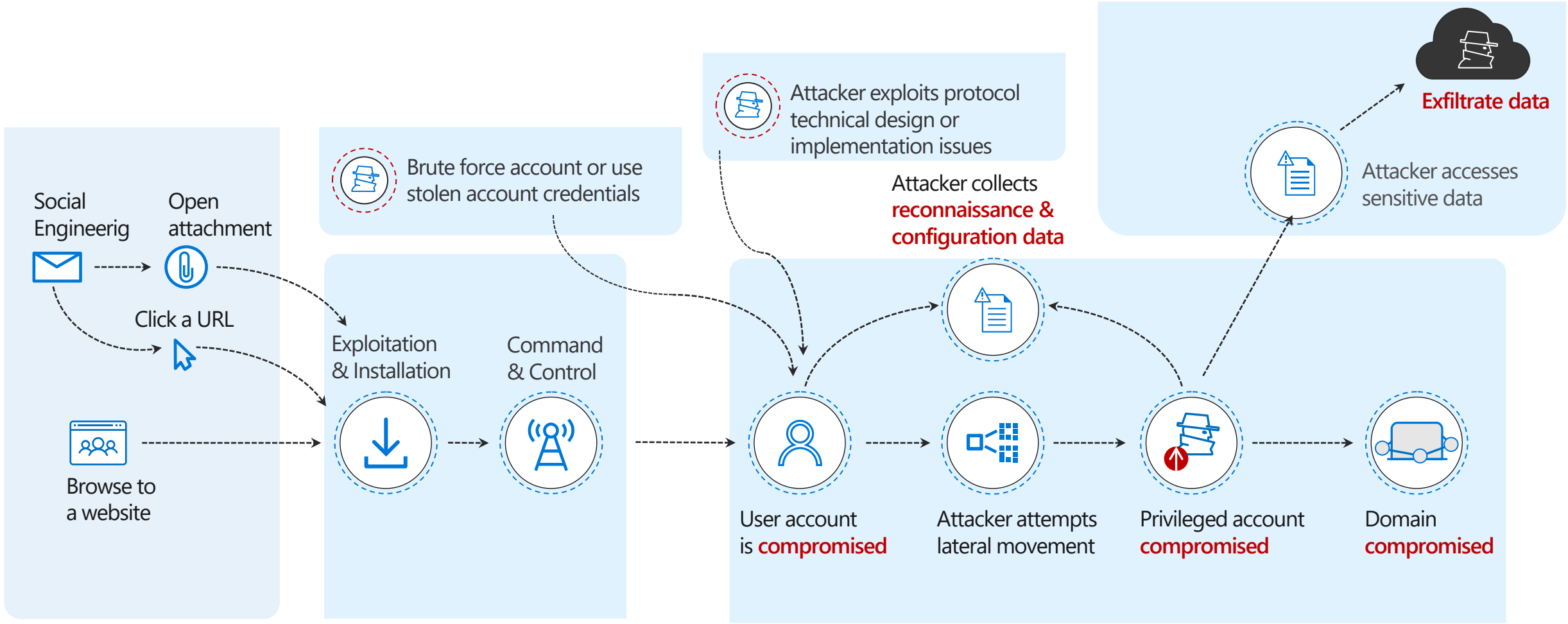
The journey (thus far)

Risk Mitigation Framework

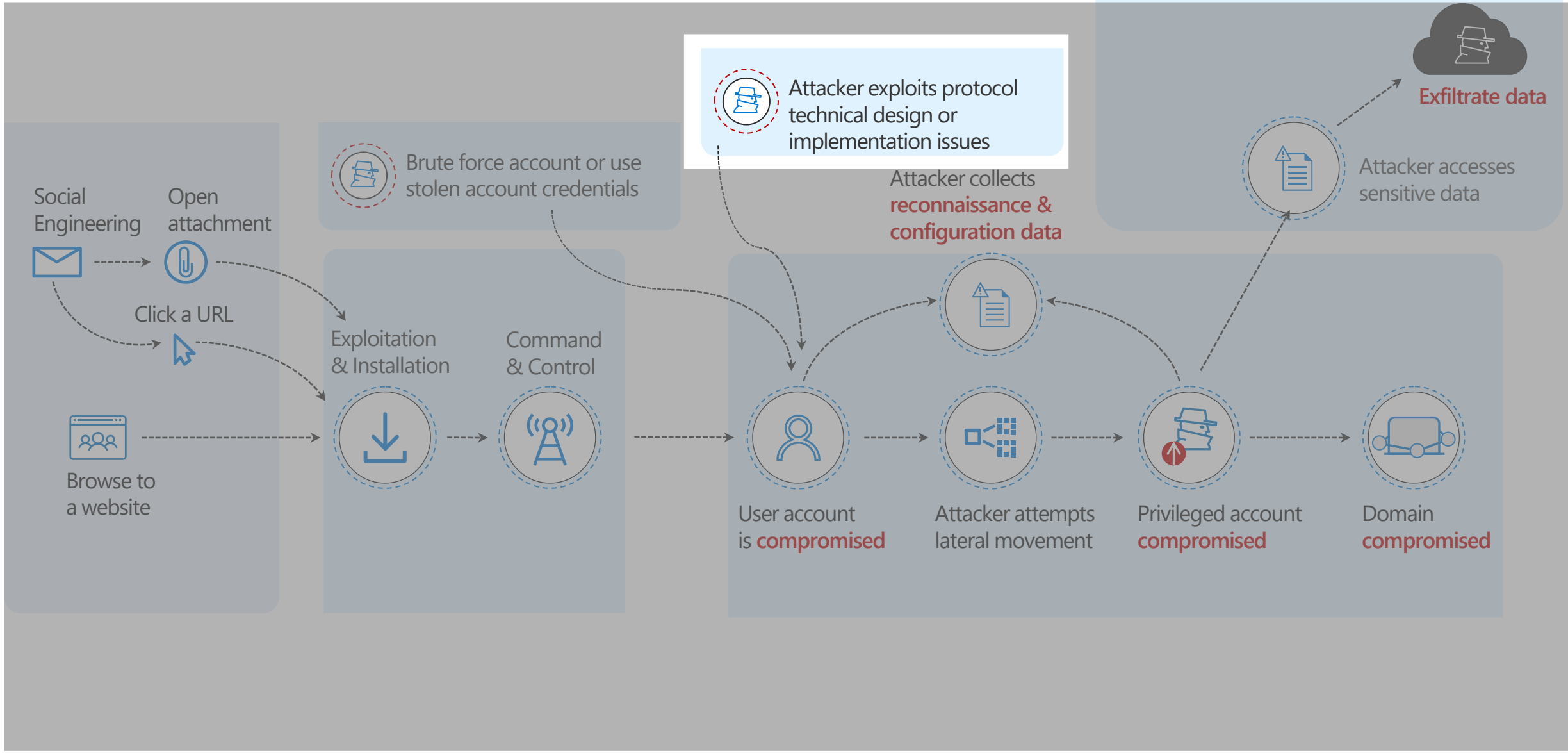
What’s in the Draft Proposal

Where we go next

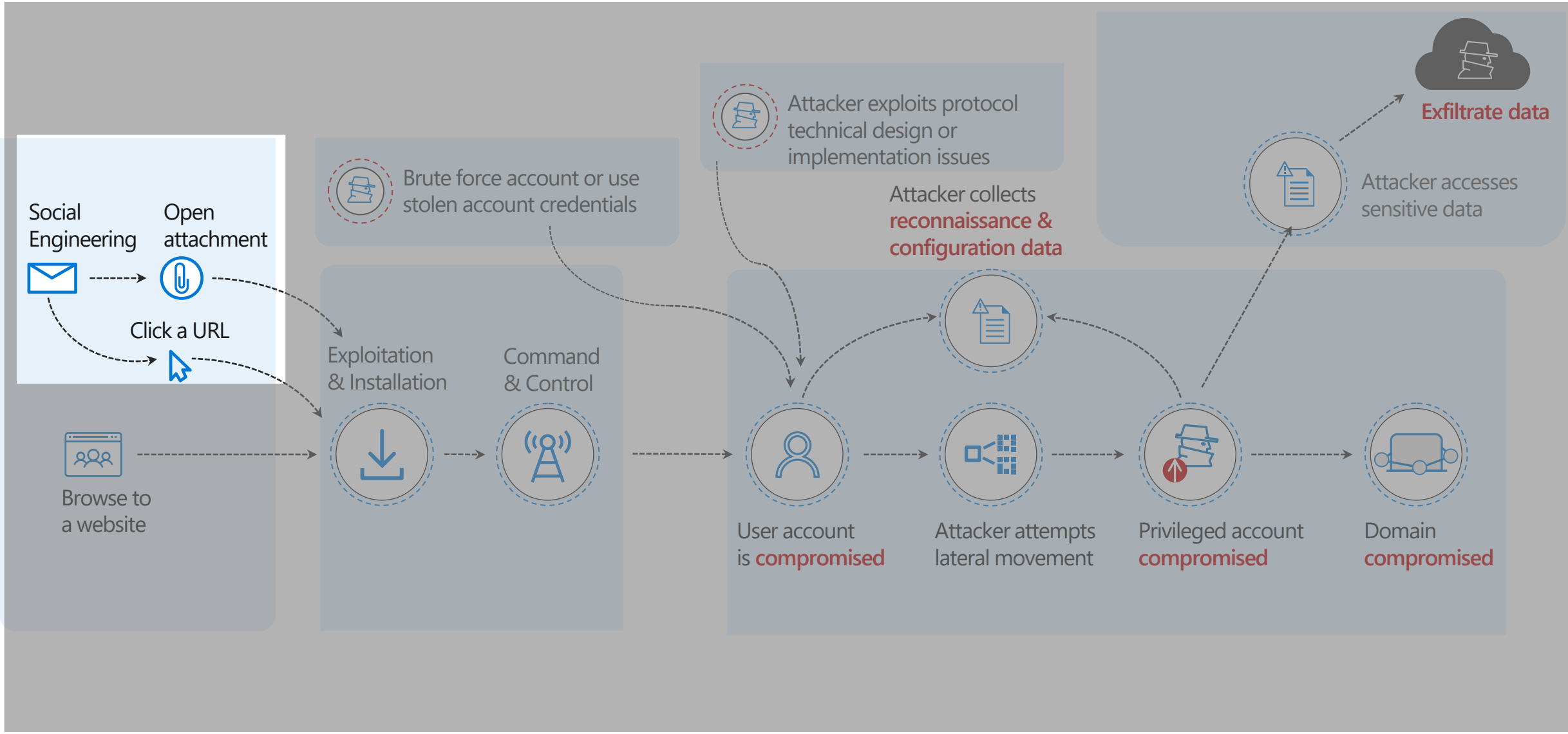
Anatomy of an attack



Where Protocol Analysts and Standards Experts Focus



Mind the Gap – Where Attackers (often) Enter



Social Engineering Exploit (1 of 5)

Attacker Controlled Device
(Initiate Session)

Authorization
Server

Endpoint

1. Get a Code

Authorization Device
(Authenticate/Authorize)

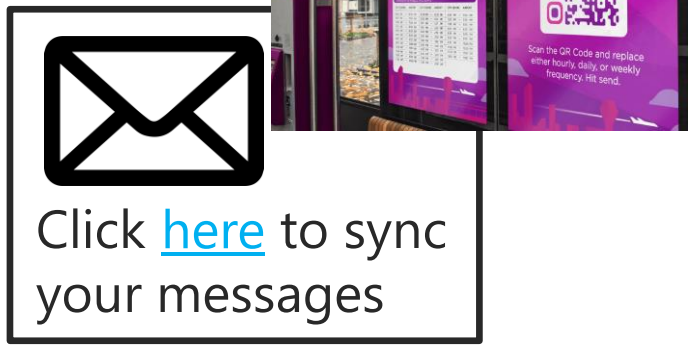
Social Engineering Exploit (2 of 5)

Authorization Server

Endpoint

1. Get a Code

Attacker Controlled Device (Initiate Session)



2. Change Context

Authorization Device (Authenticate/Authorize)

Social Engineering Exploit (3 of 5)

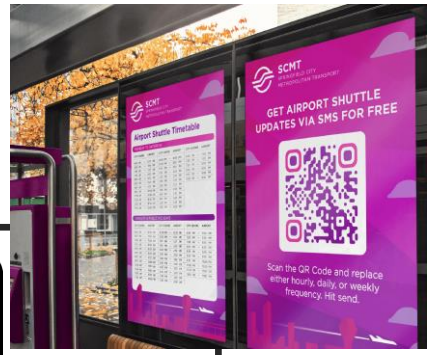
Authorization Server

Endpoint

1. Get a Code

Attacker Controlled Device (Initiate Session)

2. Change Context



3. Scan or enter a Code, click on link

Authorization Device (Authenticate/Authorize)

Social Engineering Exploit (4 of 5)

1. Get a Code

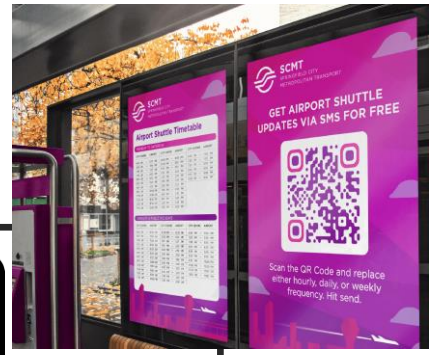
Attacker Controlled Device (Initiate Session)

Authorization Server

Endpoint

4. Authenticate/Authorize

Click here to sync your messages



2. Change Context

3. Scan or enter a Code, click on link

Authorization Device (Authenticate/Authorize)

Social Engineering Exploit (5 of 5)

5. Retrieve Tokens

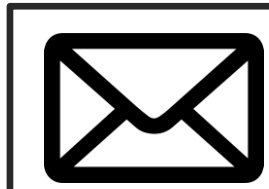
Authorization Server

Endpoint

4. Authenticate/Authorize

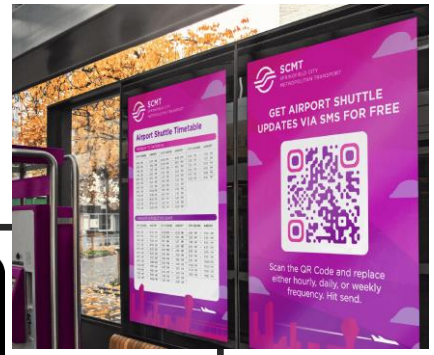
1. Get a Code

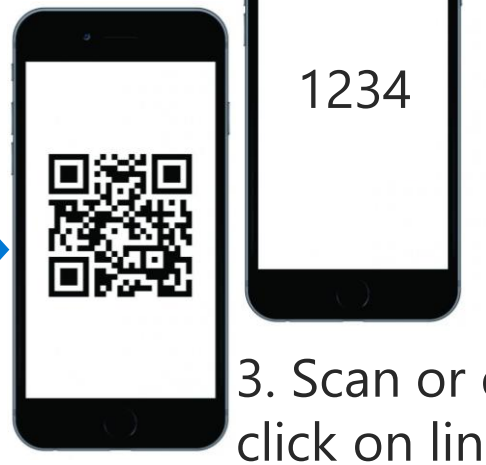
Attacker Controlled Device (Initiate Session)



Click here to sync your messages

2. Change Context





3. Scan or enter a Code, click on link

Authorization Device (Authenticate/Authorize)

Social Engineering Exploit

Authorization Server

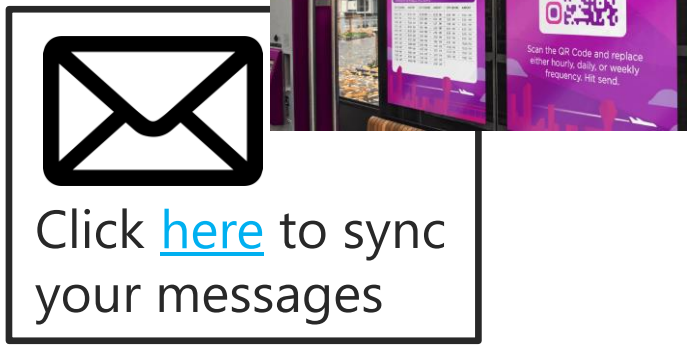
Endpoint

4. Authenticate/Authorize

5. Retrieve Tokens

1. Get a Code

Attacker Controlled Device (Initiate Session)



2. Change Context

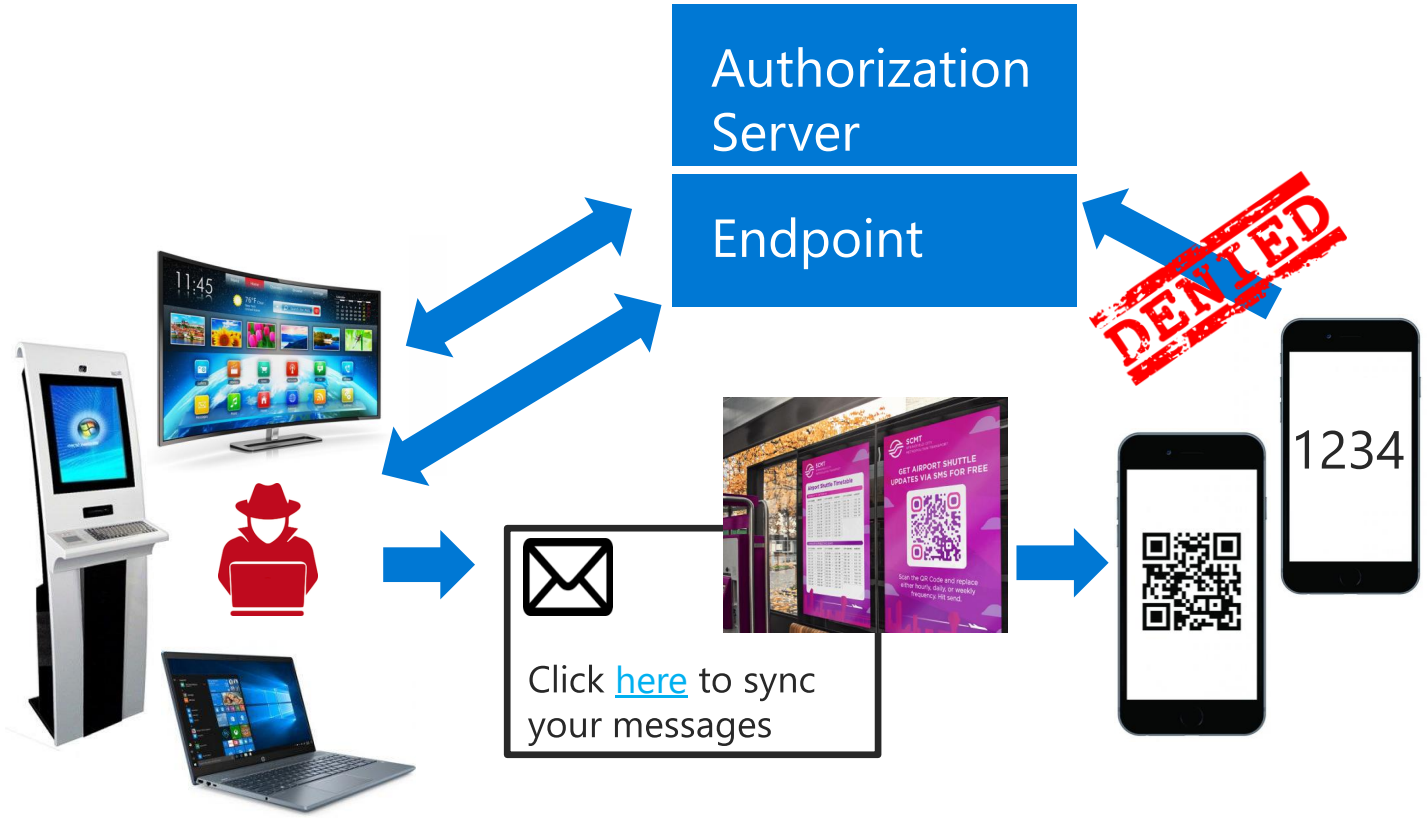
3. Scan or enter a Code, click on link

Authorization Device (Authenticate/Authorize)

Attack Pattern Summary: Exploit the Unauthenticated Channel

1. Initiate the session, retrieve code (QR code, user code)
2. Use social engineering to change context and persuade user to authorize session (illicit consent grant)
3. Bypasses multi-factor authentication (don't need to harvest credentials)

Homo Securitus to the Rescue

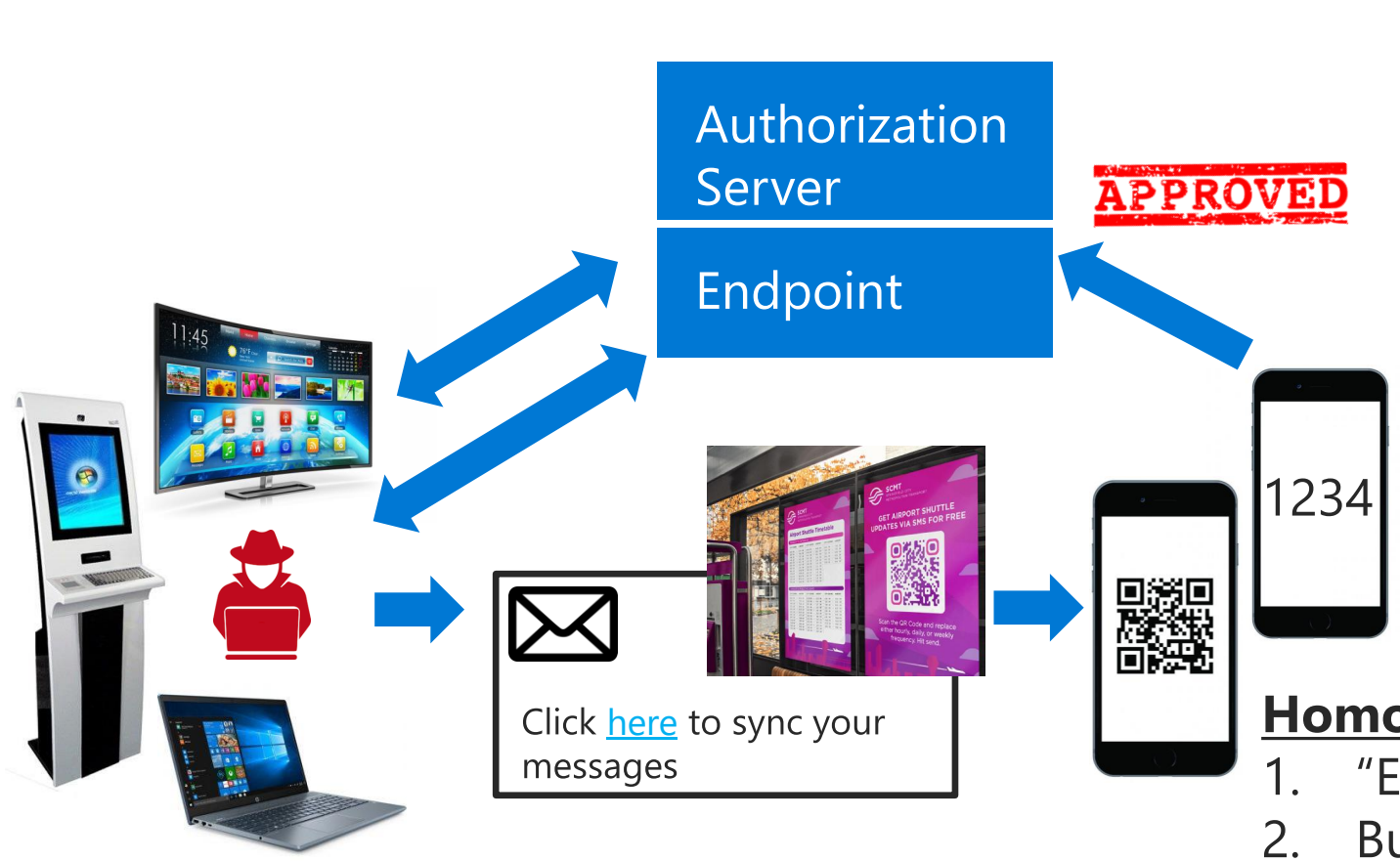


Homo Securitus

1. A security expert
2. Knows how the protocol should work
3. Detects a social engineering attempt
4. Is laser focused on current context
5. Foolproof mitigation for cross device flows

But is a rare species….

But what about Homo Sapiens?



Homo Sapiens

1. "Expertise elsewhere" - not a security expert
2. Busy and in a rush, needs to get things done
3. Worries about breaking things
4. Wants to help

Needs to make fewer decision,
Needs help to make better decisions
Needs protection even if a bad decision is made

Points to ponder…

Attacks exploit the unauthenticated channel between initiating and authorising device

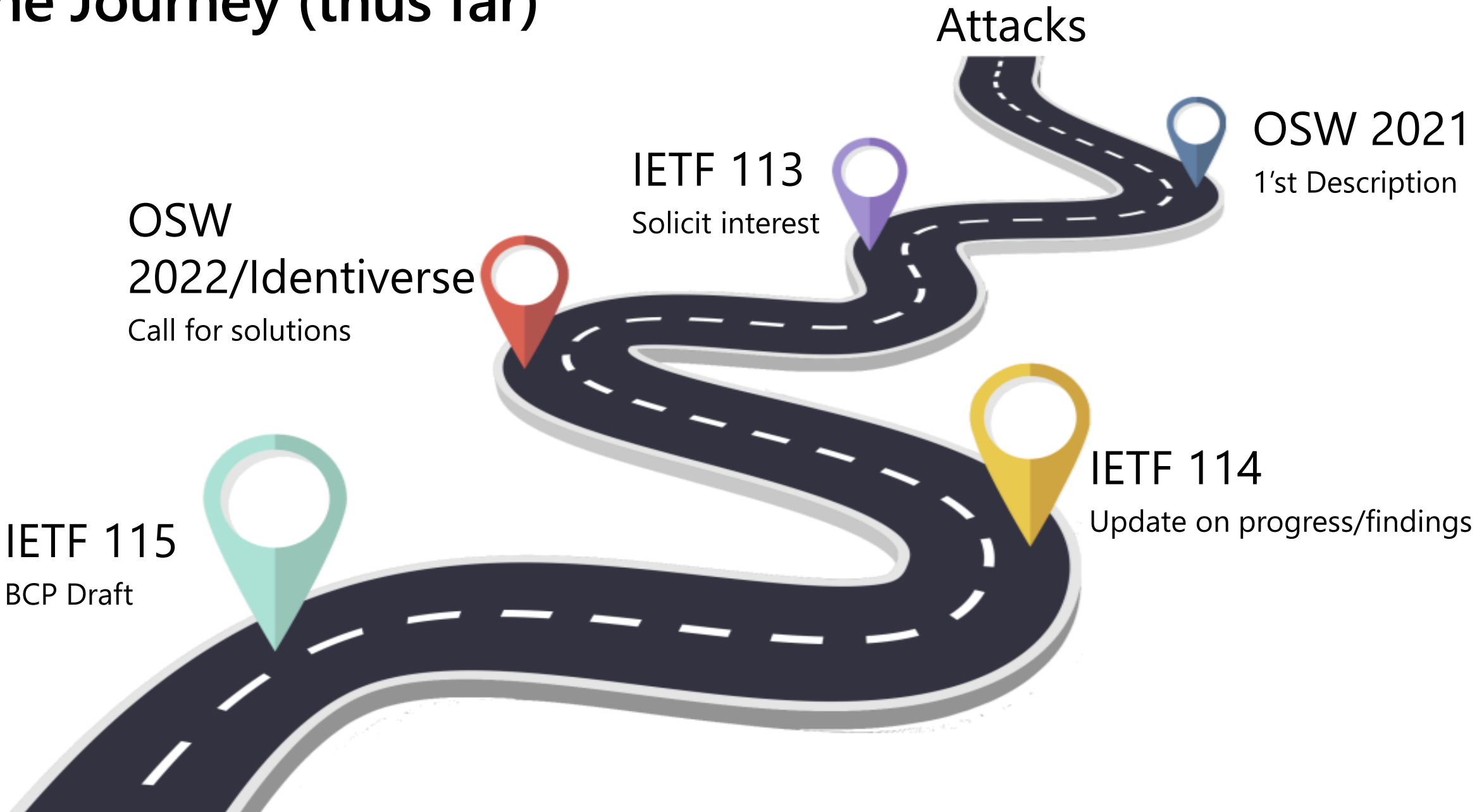
Homo Securitus vs Homo Sapiens

- Pushing responsibility on Homo Sapiens to “authenticate” the channel…

Cross Device Flows spans multiple protocols and scenarios

- Device Authorization Grant
- But also:
  - Client Initiated Backchannel Authentication (CIBA)
  - Wallet invocation (OIDF SIOP, OIDC for VCs)
  - Session transfers/Application Bootstrapping
  - Authentication (W3C WebAuthn/FIDO)

The Journey (thus far)



Mitigation Framework – Closing the Gap

Pragmatic Mitigations

- Other.....
- User Experience
- Secure QR
- Trusted Devices
- Sender Constrained Toke
- User Code Meta Data
- Content Filtering
- Proximity

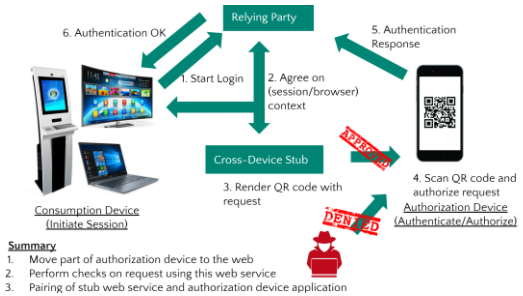
Explore Alternatives

Authenticated Channel

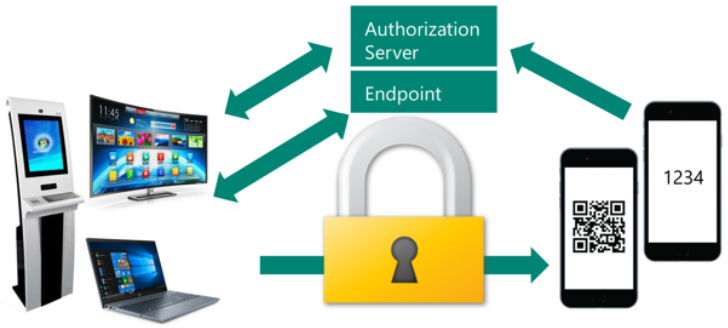
- Authorization Code Grant (WebAuthn, fido)

Unauthenticated Channel

- Client Initiated Back Channel Authentication (OpenID)
- Device Authorization Grant (OAuth 2)



Foundational Underpinnings



Draft Proposal for Cross-Device BCP

Uploaded to Datatracker: [draft-kasselman-cross-device-security-00 - Cross Device Flows: Security Best Current Practice (ietf.org)]

draft-kasselman-cross-device-security-00

Web Authorization Protocol — P. Kasselman, Microsoft
Internet-Draft — D. Fett, yes.com
Intended status: Best Current Practice — F. Skokan, Okta
Expires: 22 April 2023 — 19 October 2022

Cross Device Flows: Security Best Current Practice
draft-kasselman-cross-device-security-00

What's in the Draft Proposal: Concepts and Scenarios

2 Additional use cases suggested since publishing draft

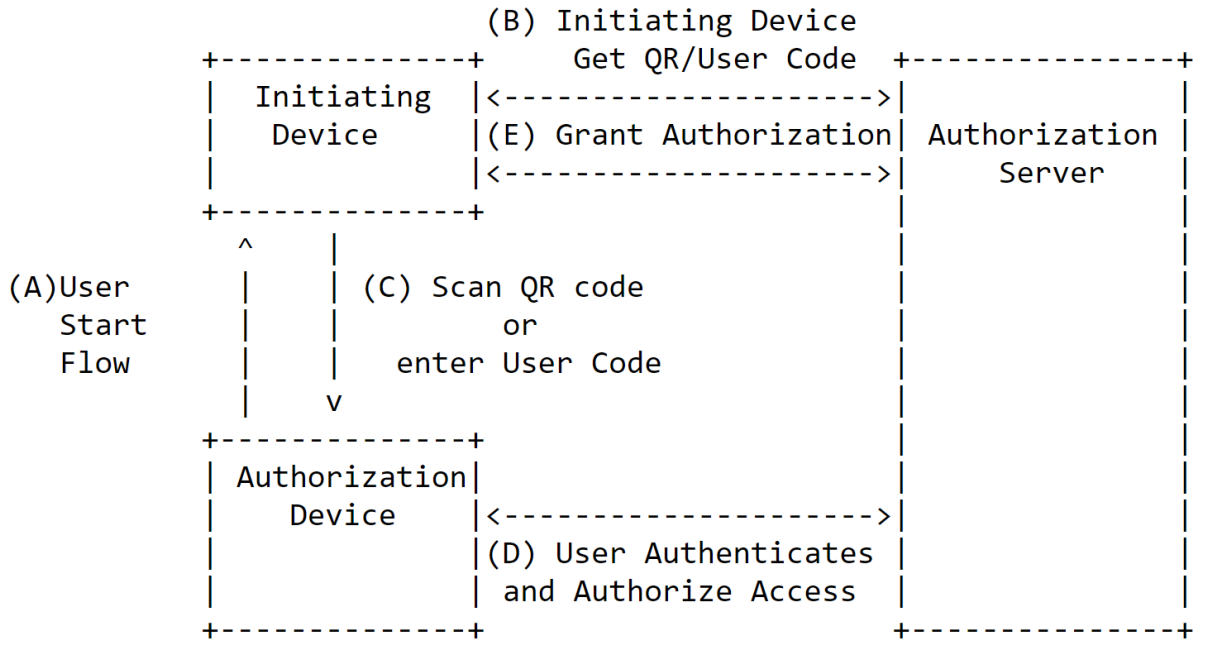


Figure 1: Typical Cross Device Flows

What's in the Draft Proposal: Attacks

1 Additional attack suggested since publishing draft

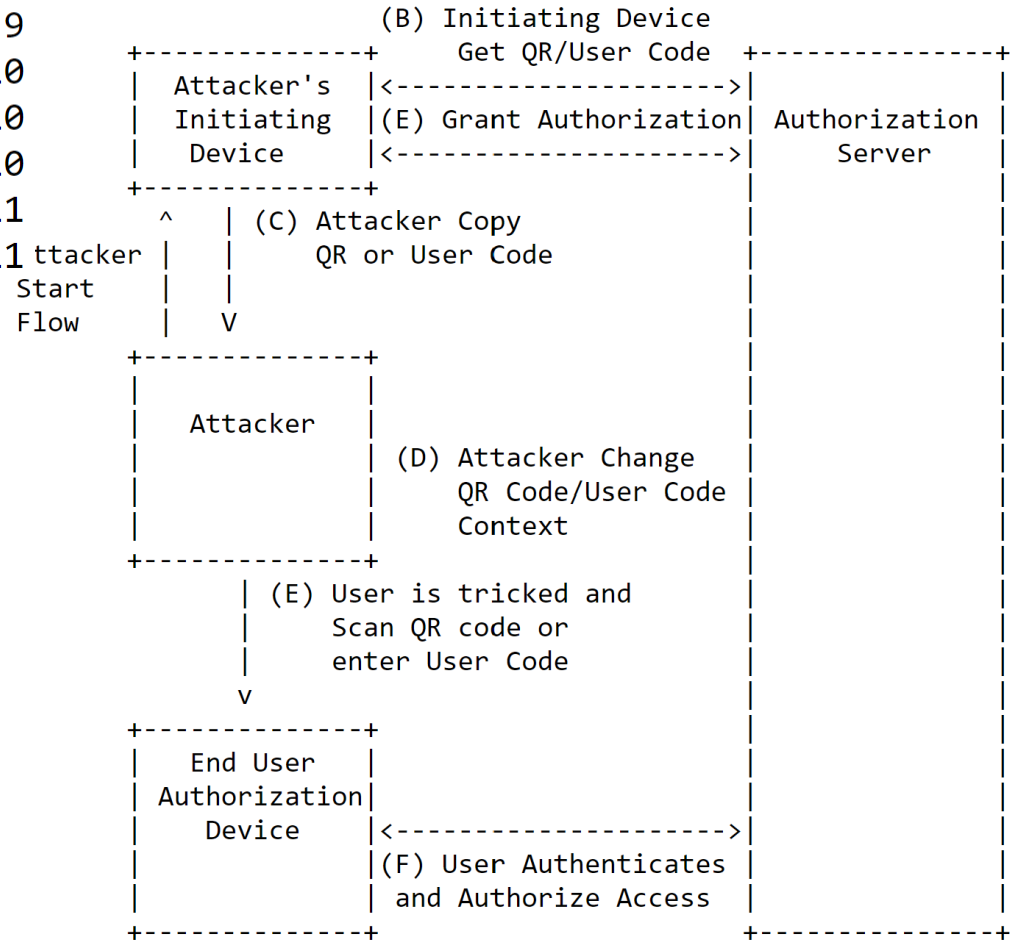


Figure 2: Typical Cross Device Flow Exploit

What's in the Draft Proposal: Mitigations

2 More community contributed mitigations since publishing draft

Mitigation	Prevent	Disrupt	Recover
Establish Proximity	X	X	
Short Lived/Timebound Codes		X	
Content Filtering		X	
Trusted Devices	X		
Trusted Networks	X		
Limited Scopes			X
Short Lived Tokens			X
Rate Limits	X	X	
Sender Constrained Tokens			X
User Experience	X		

Table 1: Practical Mitigation Summary

What's in the Draft Proposal: Protocol Selection Guidance

	Description	Susceptibility	Mitigations	Device Capabilities	When to Use
Device Authorization Grant					
Client Initiated Backchannel Authentication					
FIDO2/WebAuthn					

What's in the Draft Proposal: Foundational Pillars

Formal analysis against OAuth Protocols have been effective

Limited formal analysis of cross-device flows

- Humans are modelled as error free decision makers
- Modelling flawed decision-making may help evaluate effectiveness of mitigations

To ensure secure cross-device interactions, a formal analysis using the WIM therefore seems to be in order. Such an analysis should comprise a generic model for cross-device flows, potentially including different kinds of interactions. The aim of the analysis would be to evaluate the effectiveness of selected mitigation strategies. To the best of our knowledge, this would be the first study of this kind.

2016 IEEE 29th Computer Security Foundations Symposium

Modeling Human Errors in Security Protocols

David Basin Saša Radomirović Lara Schmid
Institute of Information Security, Department of Computer Science, ETH Zürich
Email: {david.basin, sasa.radomirovic, schmidla}@inf.ethz.ch

What Next?

Attacks

OSW 2021

1’st Description

IETF 113

Solicit interest

OSW 2022/Identiverse

Call for solutions

IETF 114

Update on progress/findings

IETF 115

BCP Draft

?